PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-286839

(43)Date of publication of application : 13.10.2000

---

(51)Int.Cl. H04L 9/32
G09C 1/00
G11B 20/10

---

(21)Application number : 11-093850 (71)Applicant : RICOH CO LTD

(22)Date of filing : 31.03.1999 (72)Inventor : KANAI YOICHI

---

(54) INFORMATION RECORDER, METHOD FOR VERIFYING AUTHENTICITY AND COMPUTER-READABLE RECORDING MEDIUM STORING PROGRAM TO ALLOW COMPUTER TO EXECUTE THE METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an information recorder, a method for verifying authenticity and a recording medium by which a value of evidence of electronic data recorded on the recording medium can efficiently be enhanced.

SOLUTION: A message authentifier generating section 104 generates a message authentifier based on media identification information specified to media such as a vendor ID, a drive ID and a disk ID stored in a PMA 110a, date and time information stored by an internal timer 102, a data recording position and electronic data and records the generated message authentifier to a CD-R medium 110 together with the electronic data.

LEGAL STATUS [Date of request for examination] 20.06.2003
[Date of sending the examiner's decision of rejection] 13.09.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection] 2005-019801
[Date of requesting appeal against examiner's decision of rejection] 13.10.2005
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] In the information recording device which verifies the bona fides of the this recorded electronic data while recording electronic data on a predetermined information record medium An authentication information calculation means to calculate authentication information based on the medium identification information of a proper to the information record medium which records electronic data, A record means to record the authentication information calculated by said authentication information calculation means on an information record medium with said electronic data, The information recording device characterized by having a verification means to verify the bona fides of said electronic data based on the authentication information recorded on said information record medium with said record means.

[Claim 2] the time check which clocks time -- the information record medium with which a means is further provided and said authentication information calculation means records electronic data -- the medium identification information of a proper, and said time check -- the information recording device according to claim 1 characterized by calculating said authentication information based on the time information which the means clocked.

[Claim 3] the information record medium with which said authentication information calculation means records electronic data at least -- the medium identification information of a proper, and said time check -- the information recording device according to claim 2 characterized by having an encryption means to encipher data including the time information which the means clocked based on predetermined cryptographic algorithm.

[Claim 4] the information record medium with which said authentication information calculation means records electronic data -- the medium identification information of a proper, and said time check -- the information recording device according to claim 3 characterized by to provide further a hash value calculation means calculate the hash value corresponding to the authentication data block which consists of the time information, the data-logging location, and the electronic data which the means clocked, and for said encryption means to encipher the hash value calculated by said hash value calculation means based on predetermined cryptographic algorithm.

[Claim 5] Said encryption means is an information recording device according to claim 4 characterized by enciphering the hash value calculated by said hash value calculation means based on the cryptographic algorithm and the predetermined private key of a public-key-encryption system.

[Claim 6] Said record means is the information recording device of any one publication

of claim 1-5 characterized by recording the authentication information which said authentication information calculation means calculated at least on the sub-code field which forms a part of each sector of said information record medium.

[Claim 7] Said information record medium is the information recording device of any one publication of claim 1-6 characterized by being the information record medium of the postscript mold which cannot perform deletion and rewriting of electronic data.

[Claim 8] Said verification means calculates new authentication information based on the medium identification information of a proper to the information record medium which recorded electronic data. The calculated new authentication information is compared with the authentication information recorded on said information record medium. The information recording device of any one publication of claim 1-7 characterized by judging that said electronic data is genuineness when both are in agreement, and judging that said electronic data is not genuineness when both are not in agreement.

[Claim 9] Said verification means compares the hash value which calculated and calculated a new hash value based on the medium identification information of a proper to the information record medium which recorded electronic data with the hash value which decoded the authentication information recorded on said information record medium. The information recording device of any one publication of claim 4-7 characterized by judging that said electronic data is genuineness when both are in agreement, and judging that said electronic data is not genuineness when both are not in agreement.

[Claim 10] It is the information recording device according to claim 9 characterized by for said encryption means recording the public key which answers the private key of a public-key-encryption system on said information record medium, and said authentication means decoding the authentication information recorded on said information record medium using the public key recorded on said information record medium.

[Claim 11] In the bona-fides verification approach of verifying the bona fides of the electronic data recorded on the predetermined information record medium The authentication information calculation process which calculates authentication information based on the medium identification information of a proper to the information record medium which records electronic data, The record process which records the authentication information calculated in said authentication information calculation process on an information record medium with said electronic data, The bona-fides verification approach characterized by including the verification process

which verifies the bona fides of said electronic data based on the authentication information recorded on said information record medium in said record process.
[Claim 12] the information record medium with which said authentication information calculation process records electronic data -- the medium identification information of a proper, and a predetermined time check -- the bona-fides verification approach according to claim 11 characterized by calculating said authentication information based on the time information which the means clocked.
[Claim 13] the information record medium with which said authentication information calculation process records electronic data at least -- the medium identification information of a proper, and said time check -- the bona-fides verification approach according to claim 12 characterized by enciphering data including the time information which the means clocked based on predetermined cryptographic algorithm.
[Claim 14] the information record medium with which said authentication information calculation process records electronic data -- the medium identification information of a proper, and said time check -- the bona-fides verification approach according to claim 13 characterized by calculating the hash value corresponding to the authentication data block which consists of the time information, the data-logging location, and electronic data which the means clocked, and enciphering the calculated hash value based on predetermined cryptographic algorithm.
[Claim 15] Said authentication information calculation process is the bona-fides verification approach according to claim 14 characterized by enciphering the hash value calculated based on the cryptographic algorithm and the predetermined private key of a public-key-encryption system.
[Claim 16] Said record process is the bona-fides verification approach of any one publication of claim 11-15 characterized by recording the authentication information calculated at said authentication information calculation process on the sub-code field which forms a part of each sector of said information record medium.
[Claim 17] Said information record medium is the bona-fides verification approach of any one publication of claim 11-16 characterized by being the information record medium of the postscript mold which cannot perform deletion and rewriting of electronic data.
[Claim 18] Said verification process calculates new authentication information based on the medium identification information of a proper to the information record medium which recorded electronic data. The calculated new authentication information is compared with the authentication information recorded on said information record medium. The bona-fides verification approach of any one publication of claim 11-17

characterized by judging that said electronic data is genuineness when both are in agreement, and judging that said electronic data is not genuineness when both are not in agreement.

[Claim 19] Said verification process compares the hash value which calculated and calculated a new hash value based on the medium identification information of a proper to the information record medium which recorded electronic data with the hash value which decoded the authentication information recorded on said information record medium. The bona-fides verification approach of any one publication of claim 14-17 characterized by judging that said electronic data is genuineness when both are in agreement, and judging that said electronic data is not genuineness when both are not in agreement.

[Claim 20] The bona-fides verification approach according to claim 19 characterized by decoding the authentication information which recorded the public key which answers the private key of a public-key-encryption system on said information record medium in said authentication information calculation process, and was recorded on said information record medium using the public key recorded on said information record medium at said authentication process.

[Claim 21] The record medium which is characterized by recording the program which makes a computer perform the approach indicated by any one of said the claims 11-20 and in which computer reading is possible.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the information recording apparatus, the bona-fides verification approach, and record medium which can heighten efficiently the sufficiency of evidence of the electronic data especially recorded on the record medium about the information recording apparatus, the bona-fides verification approach, and record medium which verify the bona fides of the this recorded electronic data while recording electronic data on a predetermined information record medium.

[0002]

[Description of the Prior Art] Conventionally, since electronic data is easy for the alteration to eliminate completely and to aim at destruction of evidence easily, this electronic data has the low value as a proof, and its certification force is low. For this reason, in order to heighten the certification force of this electronic data, it is necessary to give a digital signature (digital signature) to electronic data, or to store electronic data in the CD-R (compact disc recordable) media which are the storages of a postscript mold.

[0003] Here, this digital signature will make it requirements that (1) signature sentence cannot forge by the third person, that (2) signature sentences cannot forge by the addressee, and for a transmitting person to be unable to deny the fact of having sent (3) signature sentences later, and will transmit the signature sentence which signed with the private key which only the transmitting person knows by the public-key-encryption system to the other party. For this reason, if this digital signature is used, the certification force of electronic data will improve by the signature sentence.

[0004] Moreover, in a postscript mold storage like CD-R, even if it eliminates the electronic data recorded on CD-R media or alters, as elimination or rewriting of electronic data was made on the file system, it is only dealt with, and former electronic data remains in fact. For this reason, if this postscript mold record medium is used, since elimination of electronic data cannot be performed, the certification force of electronic data will improve.

[0005]

[Problem(s) to be Solved by the Invention] However, the above-mentioned digital signature is for proving that a certain electronic data is formed by the specific transmitting person (signer) to the last, and is not for using this electronic data as a proof. For this reason, supposing it transposes the electronic data which has the

transmitting person (signer) itself to new electronic data, even if it can check the justification of new electronic data, the proof nature of electronic data will fall.

[0006] Moreover, although the electronic data which surely was once written in CD-R media is not eliminable in a postscript mold record medium like CD-R, when copying the electronic data recorded on this postscript mold record medium to other postscript mold record media, not copying that part, then the alteration of substantial electronic data cannot be attained, and sufficiency of evidence of electronic data cannot be collateralized.

[0007] For example, five files are recorded on CD-R media, and when one of files [them] is inconvenient, the CD-R media which deleted the inconvenient file can be acquired by copying only four files which excepted the corresponding file to other CD-R media.

[0008] Thus, even if it uses a digital signature and a postscript mold record medium, since it is difficult to use electronic data as a proof, it has been a very important technical problem how the sufficiency of evidence of this electronic data is heightened.

[0009] This invention is made in view of the above-mentioned problem (technical problem), and aims at offering the information recording device, the bona-fides verification approach, and record medium which can heighten efficiently the sufficiency of evidence of the electronic data recorded on the record medium.

[0010]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, the information recording device concerning invention of claim 1 In the information recording device which verifies the bona fides of the this recorded electronic data while recording electronic data on a predetermined information record medium An authentication information calculation means to calculate authentication information based on the medium identification information of a proper to the information record medium which records electronic data, It is characterized by having a record means to record the authentication information calculated by said authentication information calculation means on an information record medium with said electronic data, and a verification means to verify the bona fides of said electronic data based on the authentication information recorded on said information record medium with said record means.

[0011] Since [according to invention of this claim 1] the bona fides of electronic data are verified based on the authentication information which recorded the authentication information which calculated and calculated authentication information

based on the medium identification information of a proper to the information record medium which records electronic data on the information record medium with said electronic data, and was recorded on the information record medium, even if it is the case where the copy between information record media is made, the bona fides of electronic data are verifiable.

[0012] moreover, the time check whose information recording apparatus concerning invention of claim 2 clocks time -- the information record medium with which a means is further provided and said authentication information calculation means records electronic data -- the medium identification information of a proper, and said time check -- it is characterized by calculating said authentication information based on the time information which the means clocked.

[0013] the information record medium which records electronic data according to invention of this claim 2 -- the medium identification information of a proper, and a time check -- since authentication information is calculated based on the time information which the means clocked, even if it is the case where a copy is performed to a just information record medium, the bona fides of electronic data are verifiable with a time stump.

[0014] moreover, the information record medium with which, as for the information recording apparatus concerning invention of claim 3, said authentication information calculation means records electronic data at least -- the medium identification information of a proper, and said time check -- it is characterized by having an encryption means to encipher data including the time information which the means clocked based on predetermined cryptographic algorithm.

[0015] the information record medium which records electronic data at least according to invention of this claim 3 -- the medium identification information of a proper, and a time check -- since [data including the time information which the means clocked] it enciphers based on predetermined cryptographic algorithm, injustice, such as an alteration of authentication information, can be prevented.

[0016] moreover, the information record medium with which, as for said authentication information calculation means, the information recording apparatus concerning invention of claim 4 records electronic data -- the medium identification information of a proper, and said time check -- a hash value calculation means calculate the hash value corresponding to the authentication data block which consists of the time information, the data-logging location, and the electronic data which a means clocked provides further, and said encryption means is characterized by to encipher the hash value calculated by said hash value calculation means based on predetermined

cryptographic algorithm.

[0017] the information record medium which records electronic data according to invention of this claim 4 -- the medium identification information of a proper, and said time check -- the hash value corresponding to the authentication data block which consists of the time information, the data-logging location, and electronic data which the means clocked is calculated, and since [the calculated hash value] it enciphers based on predetermined cryptographic algorithm, bona fides are verifiable using one index of a hash value.

[0018] Moreover, the information recording device concerning invention of claim 5 is characterized by said encryption means enciphering the hash value calculated by said hash value calculation means based on the cryptographic algorithm and the predetermined private key of a public-key-encryption system.

[0019] Since [according to invention of this claim 5] a hash value is enciphered based on the cryptographic algorithm and the predetermined private key of a public-key-encryption system, authentication information can be decoded easily.

[0020] Moreover, the information recording apparatus concerning invention of claim 6 is characterized by said record means recording the authentication information which said authentication information calculation means calculated at least on the sub-code field which forms a part of each sector of said information record medium.

[0021] The bona fides of electronic data can be verified efficiently, without changing the record format concerning an information record medium with the conventional thing, since [according to invention of this claim 6] authentication information is recorded on the sub-code field which forms a part of each sector of an information record medium at least.

[0022] Moreover, the information recording apparatus concerning invention of claim 7 is characterized by said information record medium being an information record medium of the postscript mold which cannot perform deletion and rewriting of electronic data.

[0023] According to invention of this claim 7, since the information record medium was used as the information record medium of the postscript mold which cannot perform deletion and rewriting of electronic data, it can prevent grinding of electronic data and authentication information, or **** deletion.

[0024] Moreover, the information recording device concerning invention of claim 8 Said verification means calculates new authentication information based on the medium identification information of a proper to the information record medium which recorded electronic data. When the calculated new authentication information is

compared with the authentication information recorded on said information record medium, it judges that said electronic data is genuineness when both are in agreement, and both are not in agreement, it is characterized by judging that said electronic data is not genuineness.

[0025] According to invention of this claim 8, based on the medium identification information of a proper, new authentication information is calculated to the information record medium which recorded electronic data. When the calculated new authentication information was compared with the authentication information recorded on the information record medium, it judges that electronic data is genuineness when both are in agreement, and both are not in agreement, since it judges that electronic data is not genuineness The bona fides of electronic data can be verified efficiently, without being accompanied by decode processing of authentication information.

[0026] Moreover, the information recording device concerning invention of claim 9 Said verification means compares the hash value which calculated and calculated a new hash value based on the medium identification information of a proper to the information record medium which recorded electronic data with the hash value which decoded the authentication information recorded on said information record medium. When it judges that said electronic data is genuineness when both are in agreement, and both are not in agreement, it is characterized by judging that said electronic data is not genuineness.

[0027] According to invention of this claim 9, the hash value which calculated and calculated a new hash value based on the medium identification information of a proper to the information record medium which recorded electronic data is compared with the hash value which decoded the authentication information recorded on the information record medium. When it judges that electronic data is genuineness when both are in agreement, and both are not in agreement, since it judges that electronic data is not genuineness, the bona fides of electronic data are efficiently verifiable using the index of a hash value.

[0028] Moreover, it is characterized by decoding the authentication information which recorded the public key with which said encryption means answers the private key of a public-key-encryption system in the information recording device concerning invention of claim 10 on said information record medium using the public key which recorded said authentication means on said information record medium by recording on said information record medium.

[0029] Since [according to invention of this claim 10] the authentication information

recorded on the information record medium using the public key which recorded the public key which answers the private key of a public-key-encryption system on the information record medium, and was recorded on the information record medium is decoded, it can decode and have authentication information efficiently using a public key, and the bona fides of electronic data can be verified efficiently.

[0030] Moreover, the bona-fides verification approach concerning invention of claim 11 In the bona-fides verification approach of verifying the bona fides of the electronic data recorded on the predetermined information record medium The authentication information calculation process which calculates authentication information based on the medium identification information of a proper to the information record medium which records electronic data, It is characterized by including the record process which records the authentication information calculated in said authentication information calculation process on an information record medium with said electronic data, and the verification process which verifies the bona fides of said electronic data based on the authentication information recorded on said information record medium in said record process.

[0031] Since [according to invention of this claim 11] the bona fides of electronic data are verified based on the authentication information which recorded the authentication information which calculated and calculated authentication information based on the medium identification information of a proper to the information record medium which records electronic data on the information record medium with said electronic data, and was recorded on the information record medium, even if it is the case where the copy between information record media is made, the bona fides of electronic data are verifiable.

[0032] moreover, the information record medium with which, as for said authentication information calculation process, the bona-fides verification approach concerning invention of claim 12 records electronic data -- the medium identification information of a proper, and a predetermined time check -- it is characterized by calculating said authentication information based on the time information which the means clocked.

[0033] the information record medium which records electronic data according to invention of this claim 12 -- the medium identification information of a proper, and a time check -- since authentication information is calculated based on the time information which the means clocked, even if it is the case where a copy is performed to a just information record medium, the bona fides of electronic data are verifiable with a time stump.

[0034] moreover, the information record medium with which, as for the bona-fides

verification approach concerning invention of claim 13, said authentication information calculation process records electronic data at least -- the medium identification information of a proper, and said time check -- it is characterized by enciphering data including the time information which the means clocked based on predetermined cryptographic algorithm.

[0035] the information record medium which records electronic data at least according to invention of this claim 13 -- the medium identification information of a proper, and a time check -- since [data including the time information which the means clocked] it enciphers based on predetermined cryptographic algorithm, injustice, such as an alteration of authentication information, can be prevented.

[0036] moreover, the information record medium with which, as for said authentication information calculation process, the bona-fides verification approach concerning invention of claim 14 records electronic data -- the medium identification information of a proper, and said time check -- it is characterized by to calculate the hash value corresponding to the authentication data block which consists of the time information, the data-logging location, and electronic data which the means clocked, and to encipher the calculated hash value based on predetermined cryptographic algorithm.

[0037] the information record medium which records electronic data according to invention of this claim 14 -- the medium identification information of a proper, and said time check -- the hash value corresponding to the authentication data block which consists of the time information, the data-logging location, and electronic data which the means clocked is calculated, and since [the calculated hash value] it enciphers based on predetermined cryptographic algorithm, bona fides are verifiable using one index of a hash value.

[0038] Moreover, the bona-fides verification approach concerning invention of claim 15 is characterized by said authentication information calculation process enciphering the hash value calculated based on the cryptographic algorithm and the predetermined private key of a public-key-encryption system.

[0039] Since [according to invention of this claim 15] a hash value is enciphered based on the cryptographic algorithm and the predetermined private key of a public-key-encryption system, authentication information can be decoded easily.

[0040] Moreover, the bona-fides verification approach concerning invention of claim 16 is characterized by said record process recording the authentication information calculated at said authentication information calculation process on the sub-code field which forms a part of each sector of said information record medium.

[0041] The bona fides of electronic data can be verified efficiently, without changing

the record format concerning an information record medium with the conventional thing, since [according to invention of this claim 16] authentication information is recorded on the sub-code field which forms a part of each sector of an information record medium at least.

[0042] Moreover, the bona-fides verification approach concerning invention of claim 17 is characterized by said information record medium being an information record medium of the postscript mold which cannot perform deletion and rewriting of electronic data.

[0043] According to invention of this claim 17, since the information record medium was used as the information record medium of the postscript mold which cannot perform deletion and rewriting of electronic data, it can prevent grinding of electronic data and authentication information, or **** deletion.

[0044] Moreover, the bona-fides verification approach concerning invention of claim 18 Said verification process calculates new authentication information based on the medium identification information of a proper to the information record medium which recorded electronic data. When the calculated new authentication information is compared with the authentication information recorded on said information record medium, it judges that said electronic data is genuineness when both are in agreement, and both are not in agreement, it is characterized by judging that said electronic data is not genuineness.

[0045] According to invention of this claim 18, based on the medium identification information of a proper, new authentication information is calculated to the information record medium which recorded electronic data. When the calculated new authentication information was compared with the authentication information recorded on the information record medium, it judges that electronic data is genuineness when both are in agreement, and both are not in agreement, since it judges that electronic data is not genuineness The bona fides of electronic data can be verified efficiently, without being accompanied by decode processing of authentication information.

[0046] Moreover, the bona-fides verification approach concerning invention of claim 19 Said verification process compares the hash value which calculated and calculated a new hash value based on the medium identification information of a proper to the information record medium which recorded electronic data with the hash value which decoded the authentication information recorded on said information record medium. When it judges that said electronic data is genuineness when both are in agreement, and both are not in agreement, it is characterized by judging that said electronic data

is not genuineness.

[0047] According to invention of this claim 19, the hash value which calculated and calculated a new hash value based on the medium identification information of a proper to the information record medium which recorded electronic data is compared with the hash value which decoded the authentication information recorded on the information record medium. When it judges that electronic data is genuineness when both are in agreement, and both are not in agreement, since it judges that electronic data is not genuineness, the bona fides of electronic data are efficiently verifiable using the index of a hash value.

[0048] Moreover, the bona-fides verification approach concerning invention of claim 20 is characterized by decoding the authentication information which recorded the public key which answers the private key of a public-key-encryption system on said information record medium, and was recorded on said information record medium at said authentication process using the public key recorded on said information record medium in said authentication information calculation process.

[0049] Since [according to invention of this claim 20] the authentication information recorded on the information record medium using the public key which recorded the public key which answers the private key of a public-key-encryption system on the information record medium, and was recorded on the information record medium is decoded, it can decode and have authentication information efficiently using a public key, and the bona fides of electronic data can be verified efficiently.

[0050] Moreover, the record medium concerning invention of claim 21 is having recorded the program which makes a computer perform the approach indicated by any one of said the claims 11-20, and machine reading of the program becomes possible, and it can realize actuation of claims 11-20 by computer this.

[0051]

[Embodiment of the Invention] The gestalt of suitable operation of the record medium which recorded the program which makes a computer perform the information recording device applied to this invention with reference to an accompanying drawing below, the information record approach, and its approach and in which computer reading is possible is explained to a detail. In addition, the gestalt of this operation explains the case where a CD-R drive is used as an information recording apparatus.

[0052] Drawing 1 is the functional block diagram showing the equipment configuration of the information recording apparatus used with the gestalt of this operation. The information recording apparatus 100 shown in drawing 1 heightens the sufficiency of evidence of the electronic data recorded on CD-R media by recording the message

authentication child who calculated and calculated the message authentication child based on the start-address value and day entry of electronic data in the media identification information () vendor ID of a media proper and Drive ID which were recorded on PMA(Program Memory Area)110a of the CD-R media 110, and the disk ID list on the CD-R media 110 with electronic data.

[0053] As shown in this drawing, this information recording apparatus 100 consists of the CD-R media R/W section 101, an internal timer 102, the cryptographic key Records Department 103, the message authentication child creation section 104, and a control section 105.

[0054] The CD-R media R/W section 101 is the processing section which performs writing of the electronic data to the CD-R media 110, and read-out of the electronic data from the CD-R media 110. Although this CD-R media R/W section 101 can write in electronic data in postscript to the CD-R media 110, it cannot delete the electronic data already written in the CD-R media 110.

[0055] An internal timer 102 always carries out counting of the time information, and is the processing section which outputs the time information which carried out counting to the message authentication section 104 and a control section 105 according to the demand from a control section 105.

[0056] The cryptographic key storage section 103 is the storage section which memorizes the secret cryptographic key corresponding to cryptographic algorithm, for example, when adopting conventional encryption systems, such as a DES (Data Encryption Standard) code, it memorizes the private key, and when adopting public key cryptosystems, such as a RSA (Rivest-Shamir-Adleman) code, it memorizes not a public key but a private key.

[0057] In addition, it is necessary to process the cryptographic key memorized in this cryptographic key storage section 103 so that it cannot read from the exterior. The message authentication child who creates the reason using this cryptographic key is for verifying the bona fides of electronic data, and it is because it is what only a just user should use.

[0058] The message authentication child creation section 104 is the processing section which creates the message authentication child for writing in the CD-R media 110 with electronic data, and has hash value calculation section 104a and encryption processing section 104b.

[0059] Here, this hash value calculation section 104a is the processing section which calculates a hash value with the application of predetermined hash algorithms, such as SHA-1 and MD5, to the data (henceforth an "authentication data block") which added

the start-address value and day entry of Vendor ID, Drive ID, Disk ID, and electronic data to the electronic data recorded on the CD-R media 110.

[0060] Moreover, encryption processing section 104b is the processing section enciphered with the application of predetermined cryptographic algorithm to the hash value which hash value calculation section 104a calculated using the cryptographic key memorized in the cryptographic key storage section 103. In addition, as this cryptographic algorithm, common use cryptosystems, such as a DES code, and public-key-encryption systems, such as RSA, can be used.

[0061] A control section 105 is a control section which performs control by the whole information recording apparatus 100, and when recording electronic data on the CD-R media 110, it stores in the CD-R media 110 the message authentication child who created using the above-mentioned message authentication child creation section 104 with electronic data. In addition, when electronic data is already recorded on the CD-R media 110, the bona fides of this electronic data are verified according to the procedure mentioned later.

[0062] Next, the data-logging concept with which the information recording apparatus 100 shown in drawing 1 records electronic data on the CD-R media 100 is explained. Drawing 2 is drawing showing an example of the DS of the record data which the information recording apparatus 100 shown in drawing 1 records on the CD-R media 110.

[0063] As shown in drawing 2 , one sector is formed of the electronic data 201 which actually records the usual CD-R media, and the sub-code 202 which records the control information concerning the electronic data 201. In addition, it becomes this sub-code 202 from the field and the reserve field 203 which record the address, copy information, a traffic type, etc.

[0064] For this reason, in the information recording apparatus 100 concerning this invention, message authentication child 203a which the message authentication child creation section 104 created, and time information 203b used for the creation time of this message authentication child 203a are stored in the above-mentioned reserve field 203.

[0065] Thus, in this information recording apparatus 100, since message authentication child 203a created using the information on the proper of the CD-R media 110 is stored in the CD-R media 110 with electronic data 201, the sufficiency of evidence of electronic data 201 can be heightened.

[0066] Next, the creation concept of the message authentication child by the message authentication child creation section 104 shown in drawing 1 is explained

concretely. Drawing 3 is drawing showing the creation concept of the message authentication child by the message authentication child creation section 104 shown in drawing 1 .

[0067] As shown in drawing 3 , in this message authentication child creation section 104 The vendor ID 301 of a media proper and Drive ID 302 which were recorded on PMA110a of the CD-R media 110, and a disk ID 303 With the application of a predetermined hash algorithm, a hash value 307 is calculated to the authentication data block which added a start address 304 and the time information 305 to electronic data 306. A hash value 307 is enciphered using the cryptographic key 308 and the predetermined cryptographic algorithm which were memorized in the cryptographic key storage section 103, and the message authentication child 309 is created.

[0068] For example, when using public-key-encryption systems, such as RSA, the private key is memorized in the cryptographic key storage section 103, and a hash value 307 will be enciphered using this private key. In addition, the public key in this case may be memorized on the CD-R media 110. It is because a open cryptosystem is a cryptosystem which cannot derive a private key from a public key.

[0069] Thus, in this message authentication child creation section 104, since the message authentication child 309 is created based on the vendor ID 301 of the media proper acquired from surely written-in PMA110a, drive ID 302, a disk ID 303, etc. when a CD-R drive usually formats the CD-R media 110, the CD-R media 110 can be specified as a meaning by this message authentication child 309. For this reason, even if it is the case where the partial copy of the electronic data is carried out between CD-R media, genuineness [electronic data] is verifiable using this message authentication child 309.

[0070] In addition, when the vendor ID 301 recorded on PMA110a, drive ID 302, and a disk ID 303 differ from the thing of the CD-R media which record electronic data, it can respond by adding this vendor ID 301, drive ID 302, and a disk ID 303 to the authentication data block of the CD-R media which stop record of electronic data or record electronic data.

[0071] Next, the verification procedure of the bona fides of the electronic data using this message authentication child is explained. Drawing 4 is a flow chart which shows the verification procedure of the bona fides of the electronic data using the message authentication child by the control section 105 shown in drawing 1 . In addition, electronic data shall already be stored in CD-R media with the message authentication child here.

[0072] As shown in drawing 4 , first, the information recording apparatus 100 removes

Vendor ID, Drive ID, and Disk ID from PDA110a of the CD-R media 110 (step S401), and takes out the corresponding electronic data, its message authentication child, and a day entry.

[0073] And with the application of a hash algorithm, a hash value is calculated to the data which consist of electronic data, Vendor ID, Drive ID, Disk ID, a start address, and a day entry (step S402), this hash value is enciphered and a message authentication child is calculated (step S403).

[0074] Then, the message authentication child who recorded on the calculated sub-code section of a message authentication child and the CD-R media 110 is compared (step S404), when both are in agreement, it is judged as that (Step S405 Affirmation) and whose electronic data are genuineness (step S406), and in not being in agreement, it judges that (step S405 negation) and electronic data are not intrinsic things (step S407).

[0075] Thus, also when verifying the bona fides of electronic data, the bona fides of electronic data can be verified by comparing with the message authentication child who recorded the message authentication child who created and created the message authentication child using the vendor ID memorized to PMA110a like the case where electronic data is recorded on the sub-code section of the CD-R media 110.

[0076] In addition, when verifying the bona fides of electronic data, a message authentication child cannot be created like the case where electronic data is recorded, but the message authentication child recorded on the sub-code section can be decoded, and the bona fides of electronic data can also be verified by whether the decode result is in agreement with a hash value. Since a message authentication child is decoded using the public key memorized to the CD-R media 110 and it can collate with a hash value, when encryption processing section 104b is using the algorithm of a public-key-encryption system especially, even if it does not know the cryptographic key used for a message authentication child's generation, the bona fides of data are simply verifiable.

[0077] Since it constituted from a gestalt of this operation so that the message authentication child who created and created the message authentication child based on the media identification information of media propers, such as Vendor ID, Drive ID, and Disk ID, might be recorded with electronic data as mentioned above, the unjust alteration which copies electronic data to other media can be prevented. That is, since PMA of the media proper supplied from the drive vendor of normal cannot be copied even if it copies the data on CD-R media to other media as it is, the bona fides of the electronic data by the message authentication child are verifiable.

[0078] Moreover, since not only media identification information but a day entry is considered, a message authentication child is created and a time stump becomes new even if it is the case where media identification information reproduces to right CD-R media even if, the bona fides of the electronic data by the message authentication child are verifiable.

[0079] In addition, with the gestalt of this operation, what it should be careful of here is verifying the bona fides of electronic data to the last, and is in the point of having not denied creation of backup. When a backup medium is created beforehand, though natural, a message authentication child's adjustment cannot be taken, but it is recognized, if electronic data is not necessarily inaccurate and sufficiency of evidence is inferior immediately with this.

[0080] In other words, it is sufficient to create the duplicate which has the same contents as the CD-R media of the original using this information recording apparatus 100 if CD-R media are copied like the usual procedure. In addition, media identification information (Vendor ID, Drive ID, and Disk ID) can also be recorded on the sub-code section, and it is desirable to use the cryptographic algorithm of a public-key-encryption system in that case so that the justification of a copy can be verified at a copy place in this case.

[0081] In addition, although the gestalt of the above-mentioned implementation showed the case where a message authentication child was created about all sectors, respectively, this invention is not limited to this and can also create a message authentication child for two or more sectors of every. In this case, while recording the information which shows the message authentication child for what sector it is on the reserve field of a sub-code, in case a message authentication child is calculated, it is necessary to gather the electronic data for two or more sectors as one electronic data.

[0082]

[Effect of the Invention] As explained above, according to invention of claim 1, based on the medium identification information of a proper, authentication information is calculated to the information record medium which records electronic data. Since it constituted so that the bona fides of electronic data might be verified based on the authentication information which recorded the calculated authentication information on the information record medium with said electronic data, and was recorded on the information record medium Even if it is the case where the copy between information record media is made, the effectiveness that the information recording device which can verify the bona fides of electronic data is obtained is done so.

[0083] moreover, the information record medium which records electronic data according to invention of claim 2 -- the medium identification information of a proper, and a time check -- since it constituted so that authentication information might be calculated based on the time information which the means clocked, even if it is the case where a copy is performed to a just information record medium, the effectiveness that the information recording device which can verify the bona fides of electronic data with a time stump is obtained is done so.

[0084] moreover, the information record medium which records electronic data at least according to invention of claim 3 -- the medium identification information of a proper, and a time check -- since it constituted so that data including the time information which the means clocked might be enciphered based on predetermined cryptographic algorithm, the effectiveness that the information recording device which can prevent injustice, such as an alteration of authentication information, is obtained is done so.

[0085] moreover, the information record medium which records electronic data according to invention of claim 4 -- the medium identification information of a proper, and said time check -- the hash value corresponding to the authentication data block which consists of the time information, the data-logging location, and the electronic data which the means clocked calculates, and since it constituted so that the calculated hash value may encipher based on predetermined cryptographic algorithm, the effectiveness that the information recording device which can verify bona fides using one index of a hash value is obtained does so.

[0086] Moreover, since according to invention of claim 5 it constituted so that a hash value might be enciphered based on the cryptographic algorithm and the predetermined private key of a public-key-encryption system, the effectiveness that the information recording device which can decode authentication information easily is obtained is done so.

[0087] Moreover, the effectiveness that the information recording device which can verify the bona fides of electronic data efficiently is obtained is done so, without changing the record format concerning an information record medium with the conventional thing, since according to invention of claim 6 it constituted so that authentication information might be recorded on the sub-code field which forms a part of each sector of an information record medium at least.

[0088] Moreover, according to invention of claim 7, since it constituted so that it might consider as the information record medium of the postscript mold which cannot perform deletion and rewriting of electronic data, an information record medium does

so the effectiveness that grinding of electronic data and authentication information or the information recording device which can prevent **** deletion is obtained.

[0089] Moreover, according to invention of claim 8, based on the medium identification information of a proper, new authentication information is calculated to the information record medium which recorded electronic data. Since it constituted so that it might judge that electronic data is not genuineness when the calculated new authentication information was compared with the authentication information recorded on the information record medium, it judged that electronic data is genuineness when both are in agreement, and both were not in agreement The effectiveness that the information recording device which can verify the bona fides of electronic data efficiently is obtained is done so, without being accompanied by decode processing of authentication information.

[0090] Moreover, according to invention of claim 9, the hash value which calculated and calculated a new hash value based on the medium identification information of a proper to the information record medium which recorded electronic data is compared with the hash value which decoded the authentication information recorded on the information record medium. Since it constituted so that it might judge that electronic data is not genuineness when it judged that electronic data is genuineness when both are in agreement, and both were not in agreement The effectiveness that the information recording device which can verify the bona fides of electronic data efficiently using the index of a hash value is obtained is done so.

[0091] Moreover, since it constituted according to invention of claim 10 so that the authentication information recorded on the information record medium using the public key which recorded the public key which answers the private key of a public-key-encryption system on the information record medium, and was recorded on the information record medium might be decoded, the effectiveness that the information recording device which can decode and have authentication information efficiently using a public key, and can verify the bona fides of electronic data efficiently is obtained does so.

[0092] Moreover, according to invention of claim 11, based on the medium identification information of a proper, authentication information is calculated to the information record medium which records electronic data. Since it constituted so that the bona fides of electronic data might be verified based on the authentication information which recorded the calculated authentication information on the information record medium with said electronic data, and was recorded on the information record medium Even if it is the case where the copy between information

record media is made, the effectiveness that the bona-fides verification approach that the bona fides of electronic data are verifiable is acquired is done so.

[0093] moreover, the information record medium which records electronic data according to invention of claim 12 -- the medium identification information of a proper, and a time check -- since it constituted so that authentication information might be calculated based on the time information which the means clocked, even if it is the case where a copy is performed to a just information record medium, the effectiveness that the bona-fides verification approach that the bona fides of electronic data are verifiable with a time stump is acquired is done so.

[0094] moreover, the information record medium which records electronic data at least according to invention of claim 13 -- the medium identification information of a proper, and a time check -- since it constituted so that data including the time information which the means clocked might be enciphered based on predetermined cryptographic algorithm, the effectiveness that the bona-fides verification approach that injustice, such as an alteration of authentication information, can be prevented is acquired is done so.

[0095] moreover, the information record medium which records electronic data according to invention of claim 14 -- the medium identification information of a proper, and said time check -- the hash value corresponding to the authentication data block which consists of the time information, the data-logging location, and the electronic data which the means clocked calculates, and since it constituted so that the calculated hash value may encipher based on predetermined cryptographic algorithm, the effectiveness that the bona-fides verification approach that bona fides are verifiable using one index of a hash value is acquired does so.

[0096] Moreover, since according to invention of claim 15 it constituted so that a hash value might be enciphered based on the cryptographic algorithm and the predetermined private key of a public-key-encryption system, the effectiveness that the information record medium which can decode authentication information easily is obtained is done so.

[0097] Moreover, the effectiveness that the information record medium which can verify the bona fides of electronic data efficiently is obtained is done so, without changing the record format concerning an information record medium with the conventional thing, since according to invention of claim 16 it constituted so that authentication information might be recorded on the sub-code field which forms a part of each sector of an information record medium at least.

[0098] Moreover, according to invention of claim 17, since it constituted so that it

might consider as the information record medium of the postscript mold which cannot perform deletion and rewriting of electronic data, an information record medium does so the effectiveness that grinding of electronic data and authentication information or the bona-fides verification approach that **** deletion can be prevented is acquired.

[0099] Moreover, according to invention of claim 18, based on the medium identification information of a proper, new authentication information is calculated to the information record medium which recorded electronic data. Since it constituted so that it might judge that electronic data is not genuineness when the calculated new authentication information was compared with the authentication information recorded on the information record medium, it judged that electronic data is genuineness when both are in agreement, and both were not in agreement The effectiveness that the bona-fides verification approach that the bona fides of electronic data are efficiently verifiable is acquired is done so, without being accompanied by decode processing of authentication information.

[0100] Moreover, according to invention of claim 19, based on the medium identification information of a proper, a new hash value is calculated to the information record medium which recorded electronic data. The calculated hash value is compared with the hash value which decoded the authentication information recorded on the information record medium. Since it constituted so that it might judge that electronic data is not genuineness when it judged that electronic data is genuineness when both are in agreement, and both were not in agreement The effectiveness that the bona-fides verification approach that the bona fides of electronic data are efficiently verifiable using the index of a hash value is acquired is done so.

[0101] Moreover, since according to invention of claim 20 it constituted so that the authentication information recorded on the information record medium using the public key which recorded the public key which answers the private key of a public-key-encryption system on the information record medium, and was recorded on the information record medium might be decoded, the effectiveness that the bona-fides verification approach that it can decode and have authentication information efficiently using a public key, and the bona fides of electronic data can be verified efficiently is acquired is done so.

[0102] Moreover, the record medium concerning invention of claim 21 is having recorded the program which makes a computer perform the approach indicated by any one of said the claims 11-20, and machine reading of the program becomes possible, and it can realize actuation of claims 11-20 by computer this.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the functional block diagram showing the equipment configuration of the information recording apparatus concerning the gestalt of this operation.

[Drawing 2] The information recording apparatus shown in drawing 1 is drawing showing an example of the DS of the record data recorded on CD-R media.

[Drawing 3] It is drawing showing the creation concept of the message authentication child by the message authentication child creation section shown in drawing 1 .

[Drawing 4] It is the flow chart which shows the verification procedure of the bona fides of the electronic data using the message authentication child by the control section shown in drawing 1 .

[Description of Notations]

100 Information Recording Device

101 CD-R Media

102 Internal Timer

103 Cryptographic Key Storage Section

104 Message Authentication Child Creation Section

104a Hash value calculation section

104b Encryption processing section

105 Control Section

110 CD-R Media

110a PMA

201 Electronic Data
202 Sub-code Section
203 Reserve Field
203a Time information
203b Message authentication child
301 Vendor ID
302 Drive ID
303 Disk ID
304 Start Address
305 Time Information
306 Electronic Data
307 Hash Value
308 Cryptographic Key
309 Message Authentication Child

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－286839
（P2000－286839A）
(43)公開日　平成12年10月13日(2000.10.13)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｂ	５Ｄ０４４
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ	５Ｊ１０４
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	９Ａ００１

審査請求　未請求　請求項の数21　ＯＬ　（全 12 頁）

(21)出願番号　特願平11－93850

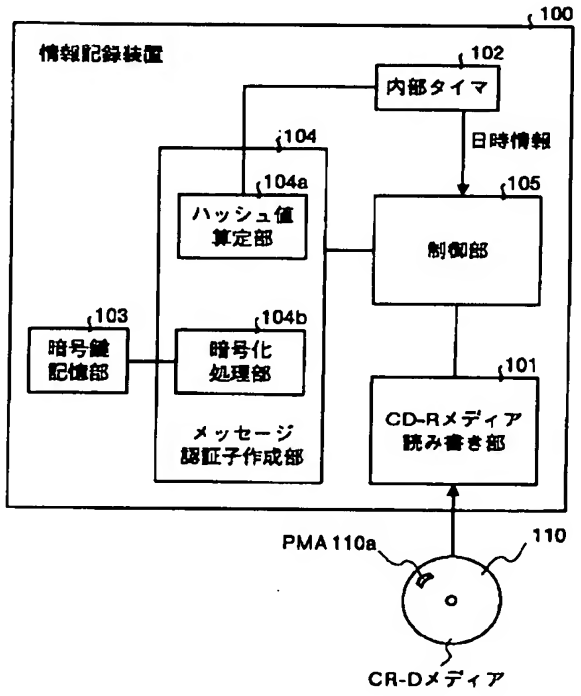
(22)出願日　平成11年３月31日(1999.3.31)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100089118
弁理士　酒井　宏明

Ｆターム(参考)　5D044 BC05 CC04 DE39 DE49 EF05
GK17
5J104 AA08 AA11 LA03 LA05 NA05
NA12 NA32 PA14
9A001 EE03 FF01 LL03

(54)【発明の名称】　情報記録装置、真正性検証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　記録媒体に記録した電子データの証拠力を効率良く高めることができる情報記録装置、真正性検証および記録媒体を提供すること。
【解決手段】　メッセージ認証子作成部１０４が、ＰＭＡ１１０ａに保持したベンダーＩＤ、ドライブＩＤおよびディスクＩＤなどのメディア固有のメディア識別情報と、内部タイマ１０２が保持する日時情報と、データ記録位置と、電子データとに基づいてメッセージ認証子を作成し、作成したメッセージ認証子を電子データとともにＣＤ－Ｒメディア１１０に記録する。



1

【特許請求の範囲】

【請求項１】　所定の情報記録媒体に電子データを記録するとともに、該記録した電子データの真正性を検証する情報記録装置において、

電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定する認証情報算定手段と、

前記認証情報算定手段により算定された認証情報を前記電子データとともに情報記録媒体に記録する記録手段と、

前記記録手段によって前記情報記録媒体に記録された認証情報に基づいて前記電子データの真正性を検証する検証手段とを備えたことを特徴とする情報記録装置。

【請求項２】　日時を計時する計時手段をさらに具備し、前記認証情報算定手段は、電子データを記録する情報記録媒体に固有の媒体識別情報と、前記計時手段が計時した日時情報とに基づいて前記認証情報を算定することを特徴とする請求項１に記載の情報記録装置。

【請求項３】　前記認証情報算定手段は、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および前記計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化する暗号化手段を備えたことを特徴とする請求項２に記載の情報記録装置。

【請求項４】　前記認証情報算定手段は、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定するハッシュ値算定手段をさらに具備し、前記暗号化手段は、前記ハッシュ値算定手段により算定されたハッシュ値を所定の暗号アルゴリズムに基づいて暗号化することを特徴とする請求項３に記載の情報記録装置。

【請求項５】　前記暗号化手段は、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいて前記ハッシュ値算定手段により算定されたハッシュ値を暗号化することを特徴とする請求項４に記載の情報記録装置。

【請求項６】　前記記録手段は、前記情報記録媒体の各セクタの一部を形成するサブコード領域に少なくとも前記認証情報算定手段が算定した認証情報を記録することを特徴とする請求項１～５のいずれか一つに記載の情報記録装置。

【請求項７】　前記情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体であることを特徴とする請求項１～６のいずれか一つに記載の情報記録装置。

【請求項８】　前記検証手段は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と前記情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする請求項１～７のいずれか一つに記載の情報記録装置。

2

【請求項９】　前記検証手段は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と前記情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする請求項４～７のいずれか一つに記載の情報記録装置。

【請求項１０】　前記暗号化手段は、公開鍵暗号系の秘密鍵に応答する公開鍵を前記情報記録媒体に記録し、前記認証手段は、前記情報記録媒体に記録した公開鍵を用いて前記情報記録媒体に記録した認証情報を復号することを特徴とする請求項９に記載の情報記録装置。

【請求項１１】　所定の情報記録媒体に記録した電子データの真正性を検証する真正性検証方法において、

電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定する認証情報算定工程と、

前記認証情報算定工程において算定された認証情報を前記電子データとともに情報記録媒体に記録する記録工程と、

前記記録工程において前記情報記録媒体に記録された認証情報に基づいて前記電子データの真正性を検証する検証工程とを含んだことを特徴とする真正性検証方法。

【請求項１２】　前記認証情報算定工程は、電子データを記録する情報記録媒体に固有の媒体識別情報と、所定の計時手段が計時した日時情報とに基づいて前記認証情報を算定することを特徴とする請求項１１に記載の真正性検証方法。

【請求項１３】　前記認証情報算定工程は、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および前記計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化することを特徴とする請求項１２に記載の真正性検証方法。

【請求項１４】　前記認証情報算定工程は、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定し、算定されたハッシュ値を所定の暗号アルゴリズムに基づいて暗号化することを特徴とする請求項１３に記載の真正性検証方法。

【請求項１５】　前記認証情報算定工程は、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいて算定されたハッシュ値を暗号化することを特徴とする請求項１４に記載の真正性検証方法。

【請求項１６】　前記記録工程は、前記情報記録媒体の各セクタの一部を形成するサブコード領域に前記認証情報算定工程で算定した認証情報を記録することを特徴とする請求項１１～１５のいずれか一つに記載の真正性検

証方法。

【請求項１７】　前記情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体であることを特徴とする請求項１１～１６のいずれか一つに記載の真正性検証方法。

【請求項１８】　前記検証工程は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と前記情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする請求項１１～１７のいずれか一つに記載の真正性検証方法。

【請求項１９】　前記検証工程は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と前記情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする請求項１４～１７のいずれか一つに記載の真正性検証方法。

【請求項２０】　前記認証情報算定工程において、公開鍵暗号系の秘密鍵に応答する公開鍵を前記情報記録媒体に記録し、前記認証工程では、前記情報記録媒体に記録した公開鍵を用いて前記情報記録媒体に記録した認証情報を復号することを特徴とする請求項１９に記載の真正性検証方法。

【請求項２１】　前記請求項１１～２０のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、所定の情報記録媒体に電子データを記録するとともに、該記録した電子データの真正性を検証する情報記録装置、真正性検証方法および記録媒体に関し、特に、記録媒体に記録した電子データの証拠力を効率良く高めることができる情報記録装置、真正性検証方法および記録媒体に関する。

【０００２】

【従来の技術】従来、電子データは、その改ざんが容易であり、また完全に消去して証拠隠滅を図ることが容易であるため、かかる電子データは証拠としての価値が低く、証明力が低い。このため、かかる電子データの証明力を高めるためには、電子データにディジタル署名（digital signature ）を施したり、追記型の記憶媒体であるＣＤ－Ｒ（compact disc recordable ）メディアなどに電子データを格納する必要がある。

【０００３】ここで、このデジタル署名とは、（１）署名文が第三者によって偽造できないこと、（２）署名文が受信者によって偽造できないこと、（３）署名文を送った事実を送信者が後で否定できないことを要件とするものであり、たとえば公開鍵暗号系では送信者のみが知っている秘密鍵で署名した署名文を相手方に送信することになる。このため、かかるデジタル署名を用いると、署名文によって電子データの証明力が向上する。

【０００４】また、ＣＤ－Ｒのような追記型記憶媒体では、ＣＤ－Ｒメディアに記録した電子データを消去したり改ざんしたとしても、ファイルシステム上で電子データの消去または書き換えがなされたように取り扱われるだけであり、実際には以前の電子データが残留する。このため、かかる追記型記録媒体を用いると、電子データの消去ができないために電子データの証明力が向上する。

【０００５】

【発明が解決しようとする課題】しかしながら、上記ディジタル署名は、あくまでもある電子データが特定の送信者（署名者）によってなされたものであることを証明するためのものであり、かかる電子データを証拠として利用するためのものではない。このため、送信者（署名者）自身がある電子データを新たな電子データに置き換えたとすると、たとえ新たな電子データの正当性を確認できても、電子データの証拠性は低下することになる。

【０００６】また、ＣＤ－Ｒのような追記型記録媒体では、確かに一旦ＣＤ－Ｒメディアに書き込んだ電子データを消去することはできないが、この追記型記録媒体に記録した電子データを他の追記型記録媒体に複写する場合に、その一部を複写しないこととすれば、実質的な電子データの改ざんが可能となり、電子データの証拠力を担保することはできない。

【０００７】たとえば、ＣＤ－Ｒメディアに５つのファイルが記録され、そのうちの１つのファイルが不都合である場合には、該当するファイルを除外した４つのファイルのみを他のＣＤ－Ｒメディアに複写することにより、不都合なファイルを削除したＣＤ－Ｒメディアを取得できることになる。

【０００８】このように、たとえディジタル署名や追記型記録媒体を用いたとしても、電子データを証拠として用いることは難しいため、かかる電子データの証拠力をいかに高めるかが極めて重要な課題となっている。

【０００９】この発明は、上記問題（課題）に鑑みてなされたものであり、記録媒体に記録した電子データの証拠力を効率良く高めることができる情報記録装置、真正性検証方法および記録媒体を提供することを目的とする。

【００１０】

【課題を解決するための手段】上記目的を達成するために、請求項１の発明に係る情報記録装置は、所定の情報記録媒体に電子データを記録するとともに、該記録した電子データの真正性を検証する情報記録装置において、

電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定する認証情報算定手段と、前記認証情報算定手段により算定された認証情報を前記電子データとともに情報記録媒体に記録する記録手段と、前記記録手段によって前記情報記録媒体に記録された認証情報に基づいて前記電子データの真正性を検証する検証手段とを備えたことを特徴とする。

【００１１】この請求項１の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定し、算定した認証情報を前記電子データとともに情報記録媒体に記録し、情報記録媒体に記録された認証情報に基づいて電子データの真正性を検証することとしたので、情報記録媒体相互間の複写がなされた場合であっても、電子データの真正性を検証することができる。

【００１２】また、請求項２の発明に係る情報記録装置は、日時を計時する計時手段をさらに具備し、前記認証情報算定手段は、電子データを記録する情報記録媒体に固有の媒体識別情報と、前記計時手段が計時した日時情報とに基づいて前記認証情報を算定することを特徴とする。

【００１３】この請求項２の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報と、計時手段が計時した日時情報とに基づいて認証情報を算定することとしたので、正当な情報記録媒体に複写がおこなわれた場合であっても、タイムスタンプにより電子データの真正性を検証することができる。

【００１４】また、請求項３の発明に係る情報記録装置は、前記認証情報算定手段は、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および前記計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化する暗号化手段を備えたことを特徴とする。

【００１５】この請求項３の発明によれば、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化することとしたので、認証情報の改ざんなどの不正を防止することができる。

【００１６】また、請求項４の発明に係る情報記録装置は、前記認証情報算定手段は、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定するハッシュ値算定手段をさらに具備し、前記暗号化手段は、前記ハッシュ値算定手段により算定されたハッシュ値を所定の暗号アルゴリズムに基づいて暗号化することを特徴とする。

【００１７】この請求項４の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定し、算定したハッシュ値を所定の暗号アルゴリズムに基づいて暗号化することとしたので、ハッシュ値という一つの指標を用いて真正性を検証することができる。

【００１８】また、請求項５の発明に係る情報記録装置は、前記暗号化手段は、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいて前記ハッシュ値算定手段により算定されたハッシュ値を暗号化することを特徴とする。

【００１９】この請求項５の発明によれば、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいてハッシュ値を暗号化することとしたので、容易に認証情報の復号をおこなうことができる。

【００２０】また、請求項６の発明に係る情報記録装置は、前記記録手段は、前記情報記録媒体の各セクタの一部を形成するサブコード領域に少なくとも前記認証情報算定手段が算定した認証情報を記録することを特徴とする。

【００２１】この請求項６の発明によれば、情報記録媒体の各セクタの一部を形成するサブコード領域に少なくとも認証情報を記録することとしたので、情報記録媒体に係る記録形式を従来のものと変えることなく、効率良く電子データの真正性を検証することができる。

【００２２】また、請求項７の発明に係る情報記録装置は、前記情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体であることを特徴とする。

【００２３】この請求項７の発明によれば、情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体としたので、電子データおよび認証情報のすりかえや削除を防止することができる。

【００２４】また、請求項８の発明に係る情報記録装置は、前記検証手段は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と前記情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする。

【００２５】この請求項８の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断することとしたので、認証情報の復号処理を伴うことなく効率良く電子データの真正性を検証することができる。

【００２６】また、請求項９の発明に係る情報記録装置は、前記検証手段は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と前記情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする。

【００２７】この請求項９の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断することとしたので、ハッシュ値という指標を用いて効率良く電子データの真正性を検証することができる。

【００２８】また、請求項１０の発明に係る情報記録装置は、前記暗号化手段は、公開鍵暗号系の秘密鍵に応答する公開鍵を前記情報記録媒体に記録し、前記認証手段は、前記情報記録媒体に記録した公開鍵を用いて前記情報記録媒体に記録した認証情報を復号することを特徴とする。

【００２９】この請求項１０の発明によれば、公開鍵暗号系の秘密鍵に応答する公開鍵を情報記録媒体に記録し、情報記録媒体に記録した公開鍵を用いて情報記録媒体に記録した認証情報を復号することとしたので、公開鍵を用いて効率良く認証情報を復号し、もって効率的に電子データの真正性を検証することができる。

【００３０】また、請求項１１の発明に係る真正性検証方法は、所定の情報記録媒体に記録した電子データの真正性を検証する真正性検証方法において、電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定する認証情報算定工程と、前記認証情報算定工程において算定された認証情報を前記電子データとともに情報記録媒体に記録する記録工程と、前記記録工程において前記情報記録媒体に記録された認証情報に基づいて前記電子データの真正性を検証する検証工程とを含んだことを特徴とする。

【００３１】この請求項１１の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定し、算定した認証情報を前記電子データとともに情報記録媒体に記録し、情報記録媒体に記録された認証情報に基づいて電子データの真正性を検証することとしたので、情報記録媒体相互間の複写がなされた場合であっても、電子データの真正性を検証することができる。

【００３２】また、請求項１２の発明に係る真正性検証方法は、前記認証情報算定工程は、電子データを記録する情報記録媒体に固有の媒体識別情報と、所定の計時手段が計時した日時情報とに基づいて前記認証情報を算定することを特徴とする。

【００３３】この請求項１２の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報と、計時手段が計時した日時情報とに基づいて認証情報を算定することとしたので、正当な情報記録媒体に複写がおこなわれた場合であっても、タイムスタンプにより電子データの真正性を検証することができる。

【００３４】また、請求項１３の発明に係る真正性検証方法は、前記認証情報算定工程は、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および前記計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化することを特徴とする。

【００３５】この請求項１３の発明によれば、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化することとしたので、認証情報の改ざんなどの不正を防止することができる。

【００３６】また、請求項１４の発明に係る真正性検証方法は、前記認証情報算定工程は、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定し、算定されたハッシュ値を所定の暗号アルゴリズムに基づいて暗号化することを特徴とする。

【００３７】この請求項１４の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定し、算定したハッシュ値を所定の暗号アルゴリズムに基づいて暗号化することとしたので、ハッシュ値という一つの指標を用いて真正性を検証することができる。

【００３８】また、請求項１５の発明に係る真正性検証方法は、前記認証情報算定工程は、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいて算定されたハッシュ値を暗号化することを特徴とする。

【００３９】この請求項１５の発明によれば、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいてハッシュ値を暗号化することとしたので、容易に認証情報の復号をおこなうことができる。

【００４０】また、請求項１６の発明に係る真正性検証方法は、前記記録工程は、前記情報記録媒体の各セクタの一部を形成するサブコード領域に前記認証情報算定工程で算定した認証情報を記録することを特徴とする。

【００４１】この請求項１６の発明によれば、情報記録媒体の各セクタの一部を形成するサブコード領域に少なくとも認証情報を記録することとしたので、情報記録媒

体に係る記録形式を従来のものと変えることなく、効率良く電子データの真正性を検証することができる。

【００４２】また、請求項１７の発明に係る真正性検証方法は、前記情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体であることを特徴とする。

【００４３】この請求項１７の発明によれば、情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体としたので、電子データおよび認証情報のすりかえや削除を防止することができる。

【００４４】また、請求項１８の発明に係る真正性検証方法は、前記検証工程は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と前記情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする。

【００４５】この請求項１８の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断することとしたので、認証情報の復号処理を伴うことなく効率良く電子データの真正性を検証することができる。

【００４６】また、請求項１９の発明に係る真正性検証方法は、前記検証工程は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と前記情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする。

【００４７】この請求項１９の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断することとしたので、ハッシュ値という指標を用いて効率良く電子データの真正性を検証することができる。

【００４８】また、請求項２０の発明に係る真正性検証方法は、前記認証情報算定工程において、公開鍵暗号系の秘密鍵に応答する公開鍵を前記情報記録媒体に記録し、前記認証工程では、前記情報記録媒体に記録した公開鍵を用いて前記情報記録媒体に記録した認証情報を復号することを特徴とする。

【００４９】この請求項２０の発明によれば、公開鍵暗号系の秘密鍵に応答する公開鍵を情報記録媒体に記録し、情報記録媒体に記録した公開鍵を用いて情報記録媒体に記録した認証情報を復号することとしたので、公開鍵を用いて効率良く認証情報を復号し、もって効率的に電子データの真正性を検証することができる。

【００５０】また、請求項２１の発明に係る記録媒体は、前記請求項１１～２０のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項１１～２０の動作をコンピュータによって実現することができる。

【００５１】

【発明の実施の形態】以下に添付図面を参照して、この発明に係る情報記録装置、情報記録方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。なお、本実施の形態では、情報記録装置としてＣＤ－Ｒドライブを用いた場合について説明する。

【００５２】図１は、本実施の形態で用いる情報記録装置の装置構成を示す機能ブロック図である。図１に示す情報記録装置１００は、ＣＤ－Ｒメディア１１０のＰＭＡ（Program Memory Area ）１１０ａに記録したメディア固有のメディア識別情報（）ベンダーＩＤ、ドライブＩＤおよびディスクＩＤ）並びに電子データの先頭アドレス値および日付情報に基づいてメッセージ認証子を算定し、算定したメッセージ認証子を電子データとともにＣＤ－Ｒメディア１１０に記録することにより、ＣＤ－Ｒメディアに記録した電子データの証拠力を高めたものである。

【００５３】同図に示すように、この情報記録装置１００は、ＣＤ－Ｒメディア読み書き部１０１と、内部タイマ１０２と、暗号鍵記録部１０３と、メッセージ認証子作成部１０４と、制御部１０５とからなる。

【００５４】ＣＤ－Ｒメディア読み書き部１０１は、ＣＤ－Ｒメディア１１０に対する電子データの書き込みと、ＣＤ－Ｒメディア１１０からの電子データの読み出しとをおこなう処理部である。このＣＤ－Ｒメディア読み書き部１０１は、ＣＤ－Ｒメディア１１０に対して電子データを追記的に書き込むことができるが、すでにＣＤ－Ｒメディア１１０に書き込んだ電子データを削除することはできない。

【００５５】内部タイマ１０２は、日時情報を常時計数し、計数した日時情報を制御部１０５からの要求に応じてメッセージ認証部１０４および制御部１０５に出力する処理部である。

【００５６】暗号鍵記憶部１０３は、暗号アルゴリズムに対応する秘密の暗号鍵を記憶する記憶部であり、たとえばＤＥＳ（Data Encryption Standard）暗号などの慣

用暗号方式を採用する場合にはその秘密鍵を記憶し、ＲＳＡ（Rivest-Shamir-Adleman）暗号などの公開鍵暗号方式を採用する場合には、パブリックキーではなくプライベートキーを記憶する。

【００５７】なお、この暗号鍵記憶部１０３に記憶する暗号鍵は、外部から読み出せないよう処理する必要がある。その理由は、かかる暗号鍵を用いて作成するメッセージ認証子は、電子データの真正性を検証するためのものであり、正当な利用者のみが使用すべきものだからである。

【００５８】メッセージ認証子作成部１０４は、電子データとともにＣＤ－Ｒメディア１１０に書き込むためのメッセージ認証子を作成する処理部であり、ハッシュ値算定部１０４ａと暗号化処理部１０４ｂとを有する。

【００５９】ここで、このハッシュ値算定部１０４ａは、ＣＤ－Ｒメディア１１０に記録する電子データに、ベンダーＩＤ、ドライブＩＤ、ディスクＩＤ、電子データの先頭アドレス値および日付情報を付加したデータ（以下「認証データブロック」と言う。）に、ＳＨＡ－１やＭＤ５などの所定のハッシュアルゴリズムを適用してハッシュ値を算定する処理部である。

【００６０】また、暗号化処理部１０４ｂは、暗号鍵記憶部１０３に記憶した暗号鍵を用いて、ハッシュ値算定部１０４ａが算定したハッシュ値に所定の暗号アルゴリズムを適用して暗号化する処理部である。なお、この暗号アルゴリズムとしては、ＤＥＳ暗号などの慣用暗号系や、ＲＳＡなどの公開鍵暗号系を使用することができる。

【００６１】制御部１０５は、情報記録装置１００の全体制御をおこなう制御部であり、ＣＤ－Ｒメディア１１０に電子データを記録する場合には、上記メッセージ認証子作成部１０４を用いて作成したメッセージ認証子を電子データとともにＣＤ－Ｒメディア１１０に格納する。なお、すでにＣＤ－Ｒメディア１１０に電子データが記録されている場合には、後述する手順にしたがってかかる電子データの真正性を検証する。

【００６２】次に、図１に示す情報記録装置１００がＣＤ－Ｒメディア１００へ電子データを記録するデータ記録概念について説明する。図２は、図１に示す情報記録装置１００がＣＤ－Ｒメディア１１０に記録する記録データのデータ構造の一例を示す図である。

【００６３】図２に示すように、通常のＣＤ－Ｒメディアは、実際に記録する電子データ２０１と、その電子データ２０１に係わる制御情報を記録するサブコード２０２とによって一つのセクタが形成される。なお、かかるサブコード２０２には、アドレス、コピー情報およびトラフィックタイプなどを記録する領域と予備領域２０３とからなる。

【００６４】このため、この発明に係わる情報記録装置１００では、メッセージ認証子作成部１０４が作成したメッセージ認証子２０３ａと、このメッセージ認証子２０３ａの作成時に用いた日時情報２０３ｂとを上記予備領域２０３に格納する。

【００６５】このように、この情報記録装置１００では、ＣＤ－Ｒメディア１１０の固有の情報を用いて作成したメッセージ認証子２０３ａを電子データ２０１とともにＣＤ－Ｒメディア１１０に格納することとしたので、電子データ２０１の証拠力を高めることができる。

【００６６】次に、図１に示すメッセージ認証子作成部１０４によるメッセージ認証子の作成概念について具体的に説明する。図３は、図１に示すメッセージ認証子作成部１０４によるメッセージ認証子の作成概念を示す図である。

【００６７】図３に示すように、かかるメッセージ認証子作成部１０４では、ＣＤ－ＲメディアＰＭＡ１１０ａに記録したメディア固有のベンダーＩＤ３０１、ドライブＩＤ３０２およびディスクＩＤ３０３と、先頭アドレス３０４および日時情報３０５とを電子データ３０６に付加した認証データブロックに所定のハッシュアルゴリズムを適用してハッシュ値３０７を算定し、暗号鍵記憶部１０３に記憶した暗号鍵３０８および所定の暗号アルゴリズムを用いてハッシュ値３０７を暗号化してメッセージ認証子３０９を作成する。

【００６８】たとえば、ＲＳＡなどの公開鍵暗号系を用いる場合には、暗号鍵記憶部１０３にプライベートキーを記憶しておき、このプライベートキーを用いてハッシュ値３０７を暗号化することになる。なお、この場合のパブリックキーは、ＣＤ－Ｒメディア１１０上に記憶してもかまわない。公開暗号系は、パブリックキーからプライベートキーを導出できない暗号系だからである。

【００６９】このように、このメッセージ認証子作成部１０４では、通常ＣＤ－ＲドライブがＣＤ－Ｒメディア１１０をフォーマットした時点で必ず書き込むＰＭＡ１１０ａから取得したメディア固有のベンダーＩＤ３０１、ドライブＩＤ３０２およびディスクＩＤ３０３などに基づいてメッセージ認証子３０９を作成しているため、かかるメッセージ認証子３０９によりＣＤ－Ｒメディア１１０は一意に特定できる。このため、ＣＤ－Ｒメディア相互間で電子データが部分複写された場合であっても、このメッセージ認証子３０９を用いて電子データが真性なものであるか否かを検証することができる。

【００７０】なお、ＰＭＡ１１０ａに記録されたベンダーＩＤ３０１、ドライブＩＤ３０２およびディスクＩＤ３０３が、電子データを記録するＣＤ－Ｒメディアのものと異なる場合には、電子データの記録を中止するか、または、電子データを記録するＣＤ－Ｒメディアの認証データブロックに、このベンダーＩＤ３０１、ドライブＩＤ３０２およびディスクＩＤ３０３を追加することにより対応することができる。

【００７１】次に、このメッセージ認証子を用いた電子

データの真正性の検証手順について説明する。図４は、図１に示す制御部１０５によるメッセージ認証子を用いた電子データの真正性の検証手順を示すフローチャートである。なお、ここではすでに電子データがメッセージ認証子とともにＣＤ－Ｒメディアに格納されているものとする。

【００７２】図４に示すように、情報記録装置１００は、まず最初に、ＣＤ－Ｒメディア１１０のＰＤＡ１１０ａからベンダーＩＤ、ドライブＩＤおよびディスクＩＤを取り出し（ステップＳ４０１）、該当する電子データとそのメッセージ認証子および日付情報とを取り出す。

【００７３】そして、電子データ、ベンダーＩＤ、ドライブＩＤ、ディスクＩＤ、先頭アドレスおよび日付情報からなるデータにハッシュアルゴリズムを適用してハッシュ値を算定し（ステップＳ４０２）、このハッシュ値を暗号化してメッセージ認証子を算定する（ステップＳ４０３）。

【００７４】その後、算定したメッセージ認証子とＣＤ－Ｒメディア１１０のサブコード部に記録したメッセージ認証子とを比較し（ステップＳ４０４）、両者が一致する場合には（ステップＳ４０５肯定）、電子データが真性であるものと判断し（ステップＳ４０６）、一致しない場合には（ステップＳ４０５否定）、電子データが真性のものではないと判断する（ステップＳ４０７）。

【００７５】このように、電子データの真正性を検証する場合にも、電子データを記録する場合と同様にしてＰＭＡ１１０ａに記憶したベンダーＩＤなどを用いてメッセージ認証子を作成し、作成したメッセージ認証子をＣＤ－Ｒメディア１１０のサブコード部に記録したメッセージ認証子と比較することにより、電子データの真正性を検証することができる。

【００７６】なお、電子データの真正性を検証する場合には、電子データを記録する場合と同様にメッセージ認証子を作成するのではなく、サブコード部に記録されたメッセージ認証子を復号し、その復号結果がハッシュ値と一致するか否かによって電子データの真正性を検証することもできる。特に、暗号化処理部１０４ｂが公開鍵暗号系のアルゴリズムを使用している場合には、ＣＤ－Ｒメディア１１０に記憶した公開鍵を用いてメッセージ認証子を復号し、ハッシュ値と照合できるため、メッセージ認証子の生成に使用した暗号鍵を知らなくとも、データの真正性を簡易に検証することができる。

【００７７】上述してきたように、本実施の形態では、ベンダーＩＤ、ドライブＩＤおよびディスクＩＤなどのメディア固有のメディア識別情報に基づいてメッセージ認証子を作成し、作成したメッセージ認証子を電子データとともに記録するよう構成したので、他のメディアに電子データを複写する不正な改ざんを防止することができる。すなわち、ＣＤ－Ｒメディア上のデータをそのまま他のメディアに複写したとしても、正規のドライブベンダーから供給されるメディア固有のＰＭＡを複写することはできないため、メッセージ認証子による電子データの真正性を検証することができる。

【００７８】また、メディア識別情報だけではなく日付情報をも加味してメッセージ認証子を作成することとしたので、たとえメディア識別情報が正しいＣＤ－Ｒメディアに複製した場合であってもタイムスタンプが新しくなってしまうため、メッセージ認証子による電子データの真正性を検証することができる。

【００７９】なお、ここで注意すべきことは、本実施の形態では、あくまでも電子データの真正性を検証しているのであって、バックアップの作成を否定しているのではないという点にある。あらかじめバックアップメディアを作成した場合には、当然ながらメッセージ認証子の整合はとれないが、このことのみによって直ちに電子データが不正であるわけではなく、証拠力が劣ると認定されるにすぎないのである。

【００８０】言い換えると、この情報記録装置１００を用いて原本のＣＤ－Ｒメディアと同じ内容を持つ複製を作成したい場合には、通常の手順と同様にしてＣＤ－Ｒメディアを複写すれば足りるのである。なお、この場合に複写先で複写の正当性を検証できるように、サブコード部にメディア識別情報（ベンダーＩＤ、ドライブＩＤおよびディスクＩＤ）を記録することもでき、その場合には、公開鍵暗号系の暗号アルゴリズムを用いることが望ましい。

【００８１】なお、上記実施の形態では、すべてのセクタについてそれぞれメッセージ認証子を作成する場合を示したが、本発明はこれに限定されるものではなく、複数のセクタごとにメッセージ認証子を作成することもできる。この場合には、何セクタ分のメッセージ認証子であるかを示す情報をサブコードの予備領域に記録するとともに、メッセージ認証子を算定する際には複数セクタ分の電子データを１つの電子データとしてまとめる必要がある。

【００８２】

【発明の効果】以上説明したように、請求項１の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定し、算定した認証情報を前記電子データとともに情報記録媒体に記録し、情報記録媒体に記録された認証情報に基づいて電子データの真正性を検証するよう構成したので、情報記録媒体相互間の複写がなされた場合であっても、電子データの真正性を検証することができる情報記録装置が得られるという効果を奏する。

【００８３】また、請求項２の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報と、計時手段が計時した日時情報とに基づいて認証情報を算定するよう構成したので、正当な情報記録媒体に複写がお

こなわれた場合であっても、タイムスタンプにより電子データの真正性を検証することができる情報記録装置が得られるという効果を奏する。

【００８４】また、請求項３の発明によれば、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化するよう構成したので、認証情報の改ざんなどの不正を防止することができる情報記録装置が得られるという効果を奏する。

【００８５】また、請求項４の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定し、算定したハッシュ値を所定の暗号アルゴリズムに基づいて暗号化するよう構成したので、ハッシュ値という一つの指標を用いて真正性を検証することができる情報記録装置が得られるという効果を奏する。

【００８６】また、請求項５の発明によれば、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいてハッシュ値を暗号化するよう構成したので、容易に認証情報の復号をおこなうことができる情報記録装置が得られるという効果を奏する。

【００８７】また、請求項６の発明によれば、情報記録媒体の各セクタの一部を形成するサブコード領域に少なくとも認証情報を記録するよう構成したので、情報記録媒体に係る記録形式を従来のものと変えることなく、効率良く電子データの真正性を検証することができる情報記録装置が得られるという効果を奏する。

【００８８】また、請求項７の発明によれば、情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体とするよう構成したので、電子データおよび認証情報のすりかえや削除を防止することができる情報記録装置が得られるという効果を奏する。

【００８９】また、請求項８の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断するよう構成したので、認証情報の復号処理を伴うことなく効率良く電子データの真正性を検証することができる情報記録装置が得られるという効果を奏する。

【００９０】また、請求項９の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断するよう構成したので、ハッシュ値という指標を用いて効率良く電子データの真正性を検証することができる情報記録装置が得られるという効果を奏する。

【００９１】また、請求項１０の発明によれば、公開鍵暗号系の秘密鍵に応答する公開鍵を情報記録媒体に記録し、情報記録媒体に記録した公開鍵を用いて情報記録媒体に記録した認証情報を復号するよう構成したので、公開鍵を用いて効率良く認証情報を復号し、もって効率的に電子データの真正性を検証することができる情報記録装置が得られるという効果を奏する。

【００９２】また、請求項１１の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定し、算定した認証情報を前記電子データとともに情報記録媒体に記録し、情報記録媒体に記録された認証情報に基づいて電子データの真正性を検証するよう構成したので、情報記録媒体相互間の複写がなされた場合であっても、電子データの真正性を検証することができる真正性検証方法が得られるという効果を奏する。

【００９３】また、請求項１２の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報と、計時手段が計時した日時情報とに基づいて認証情報を算定するよう構成したので、正当な情報記録媒体に複写がおこなわれた場合であっても、タイムスタンプにより電子データの真正性を検証することができる真正性検証方法が得られるという効果を奏する。

【００９４】また、請求項１３の発明によれば、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化するよう構成したので、認証情報の改ざんなどの不正を防止することができる真正性検証方法が得られるという効果を奏する。

【００９５】また、請求項１４の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定し、算定したハッシュ値を所定の暗号アルゴリズムに基づいて暗号化するよう構成したので、ハッシュ値という一つの指標を用いて真正性を検証することができる真正性検証方法が得られるという効果を奏する。

【００９６】また、請求項１５の発明によれば、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいてハッシュ値を暗号化するよう構成したので、容易に認証情報の復号をおこなうことができる情報記録媒体が得られるという効果を奏する。

【００９７】また、請求項１６の発明によれば、情報記録媒体の各セクタの一部を形成するサブコード領域に少なくとも認証情報を記録するよう構成したので、情報記録媒体に係る記録形式を従来のものと変えることなく、

効率良く電子データの真正性を検証することができる情報記録媒体が得られるという効果を奏する。

【００９８】また、請求項１７の発明によれば、情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体とするよう構成したので、電子データおよび認証情報のすりかえや削除を防止することができる真正性検証方法が得られるという効果を奏する。

【００９９】また、請求項１８の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断するよう構成したので、認証情報の復号処理を伴うことなく効率良く電子データの真正性を検証することができる真正性検証方法が得られるという効果を奏する。

【０１００】また、請求項１９の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断するよう構成したので、ハッシュ値という指標を用いて効率良く電子データの真正性を検証することができる真正性検証方法が得られるという効果を奏する。

【０１０１】また、請求項２０の発明によれば、公開鍵暗号系の秘密鍵に応答する公開鍵を情報記録媒体に記録し、情報記録媒体に記録した公開鍵を用いて情報記録媒体に記録した認証情報を復号するよう構成したので、公開鍵を用いて効率良く認証情報を復号し、もって効率的に電子データの真正性を検証することができる真正性検証方法が得られるという効果を奏する。

【０１０２】また、請求項２１の発明に係る記録媒体は、前記請求項１１～２０のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項１１～２０の動作をコンピュータによって実現することができる。

【図面の簡単な説明】

【図１】この実施の形態に係わる情報記録装置の装置構成を示す機能ブロック図である。

【図２】図１に示す情報記録装置がＣＤ－Ｒメディアに記録する記録データのデータ構造の一例を示す図である。

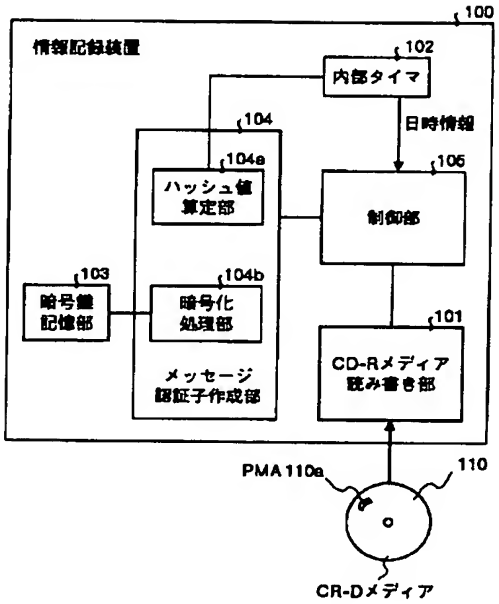
【図３】図１に示すメッセージ認証子作成部によるメッセージ認証子の作成概念を示す図である。

【図４】図１に示す制御部によるメッセージ認証子を用いた電子データの真正性の検証手順を示すフローチャートである。

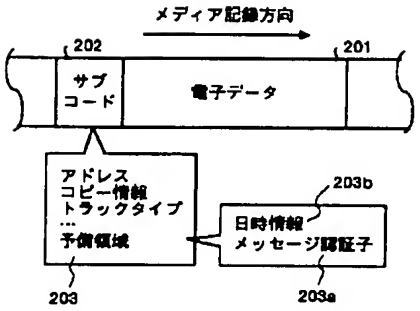
【符号の説明】

１００　情報記録装置
１０１　ＣＤ－Ｒメディア
１０２　内部タイマ
１０３　暗号鍵記憶部
１０４　メッセージ認証子作成部
１０４ａ　ハッシュ値算定部
１０４ｂ　暗号化処理部
１０５　制御部
１１０　ＣＤ－Ｒメディア
１１０ａ　ＰＭＡ
２０１　電子データ
２０２　サブコード部
２０３　予備領域
２０３ａ　日時情報
２０３ｂ　メッセージ認証子
３０１　ベンダーＩＤ
３０２　ドライブＩＤ
３０３　ディスクＩＤ
３０４　先頭アドレス
３０５　日時情報
３０６　電子データ
３０７　ハッシュ値
３０８　暗号鍵
３０９　メッセージ認証子

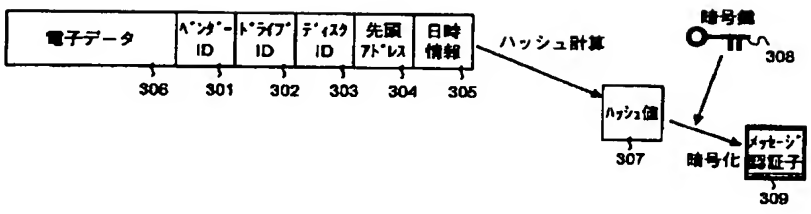
【図１】


100
情報記録装置
102
内部タイマ
日時情報
104
104a
ハッシュ値
算定部
106
制御部
103
暗号鍵
記憶部
104b
暗号化
処理部
101
CD-Rメディア
読み書き部
メッセージ
認証子作成部
PMA 110a
110
CR-Dメディア

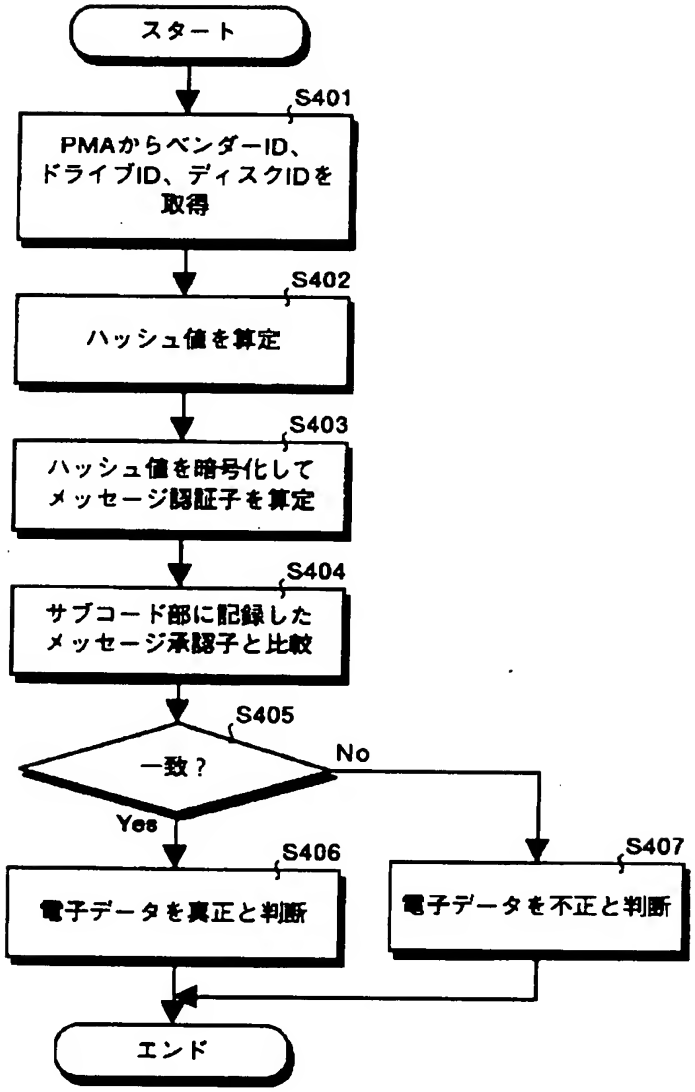
【図２】


メディア記録方向
202
201
サブ
コード
電子データ
アドレス
コピー情報
トラックタイプ
…
予備領域
203b
日時情報
メッセージ認証子
203
203a

【図３】


電子データ
ﾍﾞﾝﾀﾞｰ
ID
ﾄﾞﾗｲﾌﾞ
ID
ﾃﾞｨｽｸ
ID
先頭
ｱﾄﾞﾚｽ
日時
情報
306
301
302
303
304
305
ハッシュ計算
暗号鍵
308
ﾊｯｼｭ値
307
暗号化
ﾒｯｾｰｼﾞ
認証子
309

【図４】


スタート
S401
PMAからベンダーID、ドライブID、ディスクIDを取得
S402
ハッシュ値を算定
S403
ハッシュ値を暗号化してメッセージ認証子を算定
S404
サブコード部に記録したメッセージ承認子と比較
S405
一致？
No
Yes
S406
電子データを真正と判断
S407
電子データを不正と判断
エンド